

AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 2929
OFFERED BY MR. STEARNS

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Securely Protect Your-
3 self Against Cyber Trespass Act” or the “SPY ACT”.

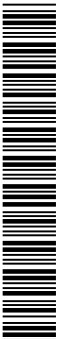
4 SEC. 2. PROHIBITION OF DECEPTIVE ACTS OR PRACTICES
5 RELATING TO SPYWARE.

6 (a) PROHIBITION.—It is unlawful for any person,
7 who is not the owner or authorized user of a protected
8 computer, to engage in deceptive acts or practices in con-
9 nection with any of the following conduct with respect to
10 the protected computer:

11 (1) Taking control of the computer by—

12 (A) utilizing such computer to send unso-
13 licited information or material from the pro-
14 tected computer to others;

15 (B) diverting the Internet browser of the
16 computer, or similar program of the computer
17 used to access and navigate the Internet, away
18 from the site the user intended to view, to one



1 or more other Web pages, such that the user is
2 prevented from viewing the content at the in-
3 tended Web page;

4 (C) accessing or using the modem, or
5 Internet connection or service, for the computer
6 and thereby causing damage to the computer or
7 causing the owner or authorized user to incur
8 unauthorized financial charges;

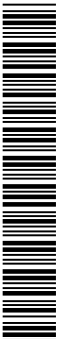
9 (D) using the computer as part of an ac-
10 tivity performed by a group of computers that
11 causes damage to another computer; or

12 (E) delivering advertisements that a user
13 of the computer cannot close without turning
14 off the computer or closing all sessions of the
15 Internet browser for the computer.

16 (2) Modifying settings related to use of the
17 computer or to the computer's access to or use of
18 the Internet by altering—

19 (A) the Web page that appears when the
20 owner or authorized user launches an Internet
21 browser or similar program used to access and
22 navigate the Internet;

23 (B) the default provider used to access or
24 search the Internet, or other existing Internet
25 connections settings;



1 (C) a list of bookmarks used by the com-
2 puter to access Web pages; or

3 (D) security or other settings of the com-
4 puter that protect information about the owner
5 or authorized user.

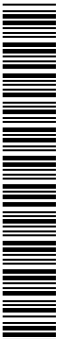
6 (3) Collecting personally identifiable informa-
7 tion through the use of a keystroke logging function
8 or similar function.

9 (4) Inducing the owner or authorized user to
10 install a computer software component onto the
11 computer, or preventing reasonable efforts to block
12 the installation or execution of, or to disable, a com-
13 puter software component by—

14 (A) presenting the owner or authorized
15 user with an option to decline installation of a
16 software component such that, when the option
17 is selected by the owner or authorized user, the
18 installation nevertheless proceeds; or

19 (B) causing a computer software compo-
20 nent that the owner or authorized user has
21 properly removed or disabled to automatically
22 reinstall or reactivate on the computer.

23 (5) Misrepresenting that installing a separate
24 software component or providing log-in and pass-
25 word information is necessary for security or privacy



1 reasons, or that installing a separate software com-
2 ponent is necessary to open, view, or play a par-
3 ticular type of content.

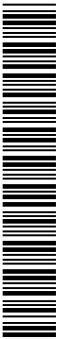
4 (6) Inducing the owner or authorized user to
5 install or execute computer software by misrep-
6 senting the identity or authority of the person or en-
7 tity providing the computer software to the owner or
8 user.

9 (7) Inducing the owner or authorized user to
10 provide personally identifiable information to an-
11 other person by misrepresenting the identity or au-
12 thority of the person seeking the information.

13 (8) Removing, disabling, or rendering inoper-
14 ative a security, anti-spyware, or anti-virus tech-
15 nology installed on the computer.

16 (9) Installing or executing on the computer one
17 or more additional computer software components
18 with the intent of causing a person to use such com-
19 ponents in a way that violates any other provision of
20 this section.

21 (b) EFFECTIVE DATE.—This section shall take effect
22 on the date of the enactment of this Act.



1 **SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFOR-**
2 **MATION WITHOUT NOTICE AND CONSENT.**

3 (a) OPT-IN REQUIREMENT.—Except as provided in
4 subsection (e), it is unlawful for any person—

5 (1) to transmit to a protected computer, which
6 is not owned by such person and for which such per-
7 son is not an authorized user, any information col-
8 lection program, or

9 (2) to execute any information collection pro-
10 gram installed on such a protected computer,
11 unless, before the first execution of any of the information
12 collection functions of the program, the owner or an au-
13 thorized user of the protected computer has consented to
14 such execution pursuant to notice in accordance with sub-
15 section (c) and such information collection program in-
16 cludes the functions required under subsection (d).

17 (b) INFORMATION COLLECTION PROGRAM.—For pur-
18 poses of this section, the term “information collection pro-
19 gram” means computer software that—

20 (1)(A) collects personally identifiable informa-
21 tion; and

22 (B)(i) sends such information to a person other
23 than the owner or authorized user of the computer,
24 or (ii) uses such information to deliver advertising
25 to, or display advertising, on the computer; or



1 (2)(A) collects information regarding the Web
2 pages accessed using the computer; and

3 (B) uses such information to deliver advertising
4 to, or display advertising on, the computer.

5 (c) NOTICE AND CONSENT.—

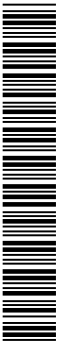
6 (1) IN GENERAL.—Notice in accordance with
7 this subsection with respect to an information collec-
8 tion program is clear and conspicuous notice in plain
9 language, set forth in a form and manner as the
10 Commission shall provide, that meets all of the fol-
11 lowing requirements:

12 (A) The notice clearly distinguishes such
13 notice from any other information visually pre-
14 sented contemporaneously on the protected
15 computer.

16 (B) The notice contains one of the fol-
17 lowing statements, as applicable, or substan-
18 tially similar language:

19 (i) With respect to an information col-
20 lection program described in subsection
21 (b)(1): “This program will collect and
22 transmit information about you. Do you
23 accept?”.

24 (ii) With respect to an information
25 collection program described in subsection



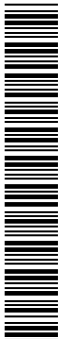
1 (b)(2): “This program will collect informa-
2 tion about Web pages you access and will
3 use that information to display advertising
4 on your computer. Do you accept?”.

5 (iii) With respect to an information
6 collection program that performs the ac-
7 tions described in both paragraphs (1) and
8 (2) of subsection (b): “This program will
9 collect and transmit information about you
10 and your computer use and will collect in-
11 formation about Web pages you access and
12 use that information to display advertising
13 on your computer. Do you accept?”.

14 (C) The notice provides for the user to
15 grant or deny consent referred to in subsection
16 (a) by selecting an option to grant or deny such
17 consent.

18 (D) The notice provides an option for the
19 user to select to display on the computer, before
20 granting or denying consent using the option
21 required under subparagraph (C), a clear de-
22 scription of—

23 (i) the types of information to be col-
24 lected and sent (if any) by the information
25 collection program;

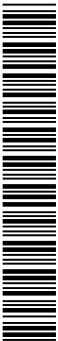


1 (ii) the purpose for which such infor-
2 mation is to be collected and sent; and

3 (iii) in the case of an information col-
4 lection program that first executes any of
5 the information collection functions of the
6 program together with the first execution
7 of other computer software, the identity of
8 any such software that is an information
9 collection program.

10 (E) The notice provides for concurrent dis-
11 play of the information required under subpara-
12 graphs (B) and (C) and the option required
13 under subparagraph (D) until the user grants
14 or denies consent using the option required
15 under subparagraph (C) (or selects the option
16 required under subparagraph (D)).

17 (2) SINGLE NOTICE.—The Commission shall
18 provide that, in the case in which multiple informa-
19 tion collection programs first execute any of the in-
20 formation collection functions of the programs to-
21 gether, notice in accordance with paragraph (1) may
22 be provided through a single notice that applies to
23 all such information collection programs, except that
24 such notice shall provide the option under subpara-



1 graph (D) of paragraph (1) with respect to each
2 such information collection program.

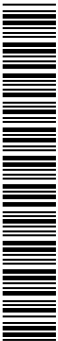
3 (3) CHANGE IN INFORMATION COLLECTED.—

4 After an owner or authorized user has granted con-
5 sent to execution of an information collection pro-
6 gram pursuant to a notice in accordance with this
7 subsection, the person who transmitted the program
8 shall provide another notice in accordance with this
9 subsection and obtain consent before such program
10 may be used to collect or send information of any
11 type or for any purpose that is materially different
12 from, and outside the scope of, the type or purpose
13 set forth in the initial or any previous notice.

14 (4) REGULATIONS.—The Commission shall
15 issue regulations to carry out this subsection.

16 (d) REQUIRED FUNCTIONS.—The functions required
17 under this subsection to be included in an information col-
18 lection program that first executes any information collec-
19 tion functions with respect to a protected computer are
20 as follows:

21 (1) DISABLING FUNCTION.—With respect to
22 any information collection program, a function of
23 the program that allows a user of the program to re-
24 move the program or disable operation of the pro-



1 gram with respect to such protected computer by a
2 function that—

3 (A) is easily identifiable to a user of the
4 computer; and

5 (B) can be performed without undue effort
6 or knowledge by the user of the protected com-
7 puter.

8 The Commission may issue regulations to carry out
9 this paragraph.

10 (2) IDENTITY FUNCTION.—With respect only to
11 an information collection program that uses informa-
12 tion collected in the manner described in paragraph
13 (1)(B)(ii) or (2)(B) of subsection (b), a function of
14 the program that provides that each display of an
15 advertisement directed or displayed using such infor-
16 mation is accompanied by a statement that clearly
17 identifies the information collection program.

18 (e) LIMITATION ON LIABILITY.—A telecommuni-
19 cations carrier, a provider of information service or inter-
20 active computer service, a cable operator, or a provider
21 of transmission capability shall not be liable under this
22 section to the extent that the carrier, operator, or
23 provider—

24 (1) transmitted, routed, hosted, stored, or pro-
25 vided connections for an information collection pro-

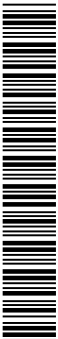


1 gram through a system or network controlled or op-
2 erated by or for the carrier, operator, or provider; or
3 (2) provided an information location tool, such
4 as a directory, index, reference, pointer, or hypertext
5 link, through which the owner or user of a protected
6 computer located an information collection program.

7 **SEC. 4. ENFORCEMENT.**

8 (a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—
9 This Act shall be enforced by the Commission under the
10 Federal Trade Commission Act (15 U.S.C. 41 et seq.).
11 A violation of any provision of this Act or of a regulation
12 issued under this Act shall be treated as an unfair or de-
13 ceptive act or practice violating a rule promulgated under
14 section 18 of the Federal Trade Commission Act (15
15 U.S.C. 57a), except that the maximum civil penalty for
16 a violation of this Act shall be one of the following
17 amounts, as the Commission, in its discretion, seeks for
18 such a violation:

19 (1) TREATMENT OF CONDUCT AFFECTING MUL-
20 TIPLE COMPUTERS AS SEPARATE VIOLATIONS.—
21 \$33,000 for each violation of section 2, and \$11,000
22 for each violation of section 3, except that in apply-
23 ing this paragraph each separate protected computer
24 with respect to which a violation of such section oc-
25 curs as a result of a single action or conduct that



1 violates section 2 or 3 shall be treated as a separate
2 violation.

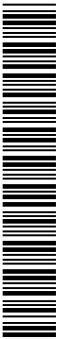
3 (2) TREATMENT OF CONDUCT AFFECTING MUL-
4 TIPLE COMPUTERS AS A SINGLE VIOLATION.—
5 \$3,000,000 for each violation of section 2, and
6 \$1,000,000 for each violation of section 3, except
7 that in applying this paragraph—

8 (A) any single action or conduct that vio-
9 lates such section with respect to multiple pro-
10 tected computers shall be treated as a single
11 violation; and

12 (B) any single action or conduct that vio-
13 lates more than one paragraph of section 2(a)
14 shall be considered multiple violations, based on
15 the number of such paragraphs violated.

16 (b) EXCLUSIVENESS OF REMEDIES.—The remedies
17 in this section (including remedies available under the
18 Federal Trade Commission Act) are the exclusive remedies
19 for violations of this Act.

20 (c) EFFECTIVE DATE.—This section shall take effect
21 on the date of the enactment of this Act, but only to the
22 extent that this section applies to violations of section
23 2(a).



1 **SEC. 5. LIMITATIONS.**

2 (a) LAW ENFORCEMENT AUTHORITY.—Sections 2
3 and 3 of this Act shall not apply to—

4 (1) any act taken by a law enforcement agent
5 in the performance of official duties; or

6 (2) the transmission or execution of an infor-
7 mation collection program in compliance with a law
8 enforcement, investigatory, national security, or reg-
9 ulatory agency or department of the United States
10 in response to a request or demand made under au-
11 thority granted to that agency or department, in-
12 cluding a warrant issued under the Federal Rules of
13 Criminal Procedure, an equivalent State warrant, a
14 court order, or other lawful process.

15 (b) EXCEPTION RELATING TO NETWORK SECU-
16 RITY.—Nothing in this Act shall apply to any monitoring
17 of, or interaction with, a subscriber's Internet or other
18 network connection or service by a telecommunications
19 carrier, cable operator, or provider of information service
20 or interactive computer service for network security pur-
21 poses, diagnostics or repair in connection with a network
22 or service, or detection or prevention of fraudulent activi-
23 ties in connection with a service or user agreement.

24 (c) GOOD SAMARITAN PROTECTION.—No provider of
25 computer software or of interactive computer service may
26 be held liable on account of any action voluntarily taken,



1 or service provided, in good faith to remove or disable a
2 program used to violate section 2 or 3 that is installed
3 on a computer of a customer of such provider, if such pro-
4 vider notifies the customer and obtains the consent of the
5 customer before undertaking such action or providing such
6 service.

7 **SEC. 6. EFFECT ON OTHER LAWS.**

8 (a) PREEMPTION OF STATE LAW.—

9 (1) PREEMPTION.—This Act supersedes any
10 provision of a statute, regulation, or rule of a State
11 or political subdivision of a State that expressly
12 regulates—

13 (A) deceptive conduct with respect to com-
14 puters similar to that described in section 2(a);

15 (B) the transmission or execution of a
16 computer program similar to that described in
17 section 3; or

18 (C) the use of context-based triggering
19 mechanisms or similar means to display an ad-
20 vertisement that partially or wholly covers or
21 obscures content on a Web page in a way that
22 interferes with the ability of the user of a com-
23 puter to view the Web page.



1 (2) PROTECTION OF CERTAIN STATE LAWS.—

2 This Act shall not be construed to preempt the ap-
3 plicability of—

4 (A) State trespass, contract, or tort law; or

5 (B) other State laws to the extent that
6 those laws relate to acts of fraud.

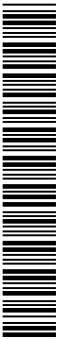
7 (b) PRESERVATION OF FTC AUTHORITY.—Nothing
8 in this Act may be construed in any way to limit or affect
9 the Commission's authority under any other provision of
10 law, including the authority to issue advisory opinions
11 (under Part 1 of Volume 16 of the Code of Federal Regu-
12 lations), policy statements, or guidance regarding this Act.

13 **SEC. 7. ANNUAL FTC REPORT.**

14 For the 12-month period that begins upon the effec-
15 tive date under section 10(a) and for each 12-month pe-
16 riod thereafter, the Commission shall submit a report to
17 the Congress that—

18 (1) specifies the number and types of actions
19 taken during such period to enforce sections 2(a)
20 and 3, the disposition of each such action, any pen-
21 alties levied in connection with such actions, and any
22 penalties collected in connection with such actions;
23 and

24 (2) describes the administrative structure and
25 personnel and other resources committed by the



1 Commission for enforcement of this Act during such
2 period.

3 Each report under this subsection for a 12-month period
4 shall be submitted not later than 90 days after the expira-
5 tion of such period.

6 **SEC. 8. REGULATIONS.**

7 Any regulations issued pursuant to this Act shall be
8 issued in accordance with section 553 of title 5, United
9 States Code, not later than the expiration of the 6-month
10 period beginning on the date of the enactment of this Act.

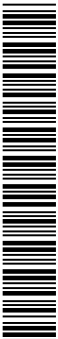
11 **SEC. 9. DEFINITIONS.**

12 For purposes of this Act:

13 (1) CABLE OPERATOR.—The term “cable oper-
14 ator” has the meaning given such term in section
15 602 of the Communications Act of 1934 (47 U.S.C.
16 522).

17 (2) COLLECT.—The term “collect” means, with
18 respect to information and for purposes only of sec-
19 tion 3, to obtain in a manner other than by transfer
20 by an owner or authorized user of a protected com-
21 puter to the party intended as recipient of the trans-
22 ferred information.

23 (3) COMPUTER; PROTECTED COMPUTER.—The
24 terms “computer” and “protected computer” have



1 the meanings given such terms in section 1030(e) of
2 title 18, United States Code.

3 (4) COMPUTER SOFTWARE.—

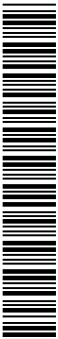
4 (A) IN GENERAL.—Except as provided in
5 subparagraph (B), the term “computer soft-
6 ware” means a set of statements or instructions
7 that can be installed and executed on a com-
8 puter for the purpose of bringing about a cer-
9 tain result.

10 (B) EXCEPTION FOR COOKIES.—Such term
11 does not include a cookie or other text file,
12 data, or computer software, that is placed on
13 the computer system of a user by an Internet
14 service provider, interactive computer service, or
15 Internet website to return information to such
16 provider, service, or website solely to enable the
17 user subsequently to use such provider or serv-
18 ice or to access such website.

19 (5) COMMISSION.—The term “Commission”
20 means the Federal Trade Commission.

21 (6) DAMAGE.—The term “damage” has the
22 meaning given such term in section 1030(e) of title
23 18, United States Code.

24 (7) DECEPTIVE ACTS OR PRACTICES.—The
25 term “deceptive acts or practices” has the meaning



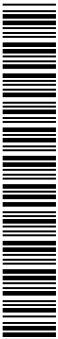
1 applicable to such term for purposes of section 5 of
2 the Federal Trade Commission Act (15 U.S.C. 45).

3 (8) DISABLE.—The term ‘disable’ means, with
4 respect to an information collection program, to per-
5 manently prevent such program from executing any
6 of the functions described in section 3(b) that such
7 program is otherwise capable of executing (including
8 by removing, deleting, or disabling the program), un-
9 less the owner or operator of a protected computer
10 takes a subsequent affirmative action to enable the
11 execution of such functions.

12 (9) INFORMATION COLLECTION FUNCTIONS.—
13 The term “information collection functions” means,
14 with respect to an information collection program,
15 the functions of the program described in subsection
16 (b) of section 3.

17 (10) INFORMATION SERVICE.—The term “infor-
18 mation service” has the meaning given such term in
19 section 3 of the Communications Act of 1934 (47
20 U.S.C. 153).

21 (11) INTERACTIVE COMPUTER SERVICE.—The
22 term “interactive computer service ” has the mean-
23 ing given such term in section 230(f) of the Commu-
24 nications Act of 1934 (47 U.S.C. 230(f)).



1 (12) INTERNET.—The term “Internet” means
2 collectively the myriad of computer and tele-
3 communications facilities, including equipment and
4 operating software, which comprise the inter-
5 connected world-wide network of networks that em-
6 ploy the Transmission Control Protocol/Internet
7 Protocol, or any predecessor or successor protocols
8 to such protocol, to communicate information of all
9 kinds by wire or radio.

10 (13) PERSONALLY IDENTIFIABLE INFORMA-
11 TION.—

12 (A) IN GENERAL.—The term “personally
13 identifiable information” means the following
14 information, to the extent only that such infor-
15 mation allows a living individual to be identified
16 from that information:

17 (i) First and last name of an indi-
18 vidual.

19 (ii) A home or other physical address
20 of an individual, including street name,
21 name of a city or town, and zip code.

22 (iii) An electronic mail address.

23 (iv) A telephone number.

24 (v) A social security number, tax iden-
25 tification number, passport number, driv-



1 er's license number, or any other govern-
2 ment-issued identification number.

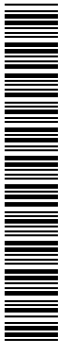
3 (vi) A credit card number.

4 (vii) An account number.

5 (viii) Any access code or password,
6 other than an access code or password
7 transmitted by an owner or authorized
8 user of a protected computer to register
9 for, or log onto, a Web page or other
10 Internet service that is protected by an ac-
11 cess code or password.

12 (ix) Date of birth, birth certificate
13 number, or place of birth of an individual,
14 except in the case of a date of birth re-
15 quired by law to be transmitted or col-
16 lected.

17 (B) RULEMAKING.—The Commission may,
18 by regulation, add to the types of information
19 specified under paragraph (1) that shall be con-
20 sidered personally identifiable information for
21 purposes of this Act, except that such informa-
22 tion may not include any record of aggregate
23 data that does not identify particular persons,
24 particular computers, particular users of com-
25 puters, or particular email addresses or other



1 locations of computers with respect to the
2 Internet.

3 (14) TELECOMMUNICATIONS CARRIER.—The
4 term “telecommunications carrier” has the meaning
5 given such term in section 3 of the Communications
6 Act of 1934 (47 U.S.C. 153).

7 (15) TRANSMIT.—The term “transmit” means,
8 with respect to an information collection program,
9 transmission by any means.

10 (16) WEB PAGE.—The term “Web page” means
11 a location, with respect to the World Wide Web, that
12 has a single Uniform Resource Locator or another
13 single location with respect to the Internet, as the
14 Federal Trade Commission may prescribe.

15 **SEC. 10. APPLICABILITY AND SUNSET.**

16 (a) EFFECTIVE DATE.—Except as specifically pro-
17 vided otherwise in this Act, this Act shall take effect upon
18 the expiration of the 12-month period that begins on the
19 date of the enactment of this Act.

20 (b) APPLICABILITY.—Section 3 shall not apply to an
21 information collection program installed on a protected
22 computer before the effective date under subsection (a) of
23 this section.

24 (c) SUNSET.—This Act shall not apply after Decem-
25 ber 31, 2009.

